Ing. et Ing. Jiří Konečný, Ph.D.
Ing. Martina Janková, BA (Hons)
prof. Ing. Jiří Dvořák, DrSc.
Ing. Vladimír Šulc, Ph.D.

# Modely systémově vymezených procesů pro kybernetickou bezpečnost

Models of Systemically Defined Processes for Cybersecurity

*ABSTRAKT: V tomto příspěvku vycházíme z dílčích závěrů výzkumných úkolů pracovišť a z podrobné analýzy informačních zdrojů specifického výzkumu. Je zde uveden závěr zásadního systémového vymezení procesů v nově pojaté výuce kybernetické bezpečnosti na fakultě a to z pohledu nově přijatého zákona a potřeb vysokoškolské výuky kybernetické bezpečnosti v ČR. Pozornost je věnována zcela novému pojetí laboratoří aplikované kybernetiky. Je zde uvedena koncepce výstavby této laboratoře složené z pracovišť kybernetických útoků, kybernetické obrany, kybernetické bezpečnosti a tomu odpovídajícího centra pro znalostní pracovníky kybernetické bezpečnosti. Toto centrum bude sloužit kvalifikovaným znalostním pracovníkům k získávání informací k řešeným aktuálním otázkám bezpečnosti modelů reálných podniků a organizací z pohledu technického a potřebného právního prostředí. Informační a komunikační technologie (instalovaný internet a komunikační prostředky) mohou přispět k práci soudních znalců v této kybernetické bezpečnosti.*

*KLÍČOVÁ SLOVA: procesní inženýrství, kybernetický prostor, kybernetická bezpečnost, model a modelování systémů, soudní inženýrství*

*ABSTRACT: In this paper we build on partial conclusions of department research projects and on a detailed analysis of information sources for specific research. There is stated a conclusion of fundamental systemic definition of processes in the new approach to teaching cyber security at the faculty and all that from the perspective of the newly adopted law and needs of university education of cyber security in the Czech Republic. Attention is paid to an entirely new concept of laboratories for Applied Cybernetics. There is presented a concept for constructing this laboratory which is composed from workplaces of cyber attacks, cyber defence, cyber security and a corresponding centre for knowledge workers of cyber security. This centre will serve to qualified knowledge workers to obtain information about currently being solved questions for security models of real companies and organizations from a point of view of technical and the necessary legal environment. Information and communication technology (installed Internet and communication devices) may contribute to the work of judicial experts in this cyber security.*

*KEYWORDS: process engineering, cyberspace, cyber security, model and systems modelling, forensic engineering*

## 1. ÚVOD

Světová nově pojatá „*technologická revoluce*" je podmíněna rychlým vývojem moderní informatiky (informačních a komunikačních technologií – ICT), kybernetiky (kybernetických strojů jako jsou numericky řízené stroje, roboty a robotické linky, roboty s umělou inteligencí, učící se systémy a „*učící se organizace a podniky*"). Především [2] vše na pozadí nových poznatků moderní fyziky, moderní matematiky, teorie systémů a kybernetiky, filosofie, práva, procesního inženýrství a samozřejmě především teoretických a také praktických nástrojů vhodných pro tvorbu modelů procesů systémově vymezených a modelování složitých systémů. Samozřejmě také principů simulace a používání nově pojatých osnov vysokoškolského studia a celoživotního vzdělávání znalostních pracovníků v moderních firmách a organizacích. Samozřejmostí má být využívání moderních inteligentních laboratoří a postupné užívání, ve světě již uznávaných, simulátorů v novém kybernetickém prostoru. Vše s novými přístupy v „*aplikované kybernetice*", „*technické kybernetice*" a prostředích „*umělé inteligence*". A také nového pojetí oblastí charakterizovaných procesy moderních kybernetických útoků a obrany systémů a integrující kybernetické bezpečnosti před prostředky, již probíhající kybernetické války ve světě. Nové pojetí kybernetického prostoru (kyberprostoru) a v něm vyrůstající nové „*učící se organizace*" dává také nový

*Dodáno autory do redakce 9. 2. 2017. • Recenzní řízení od 13. 2. do 10. 3. 2017.*

*Ing. et Ing. Jiří Konečný, Ph.D., Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení, Ústav krizového řízení, Studentské nám. 1532, 686 01 Uherské Hradiště, e-mail: konecny@flkr.utb.cz*
*Ing. Martina Janková, BA (Hons), Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky, Kolejní 2906/4, 612 00 Brno, e-mail: martina.jankova@email.cz*
*Prof. Ing. Jiří Dvořák, DrSc., Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení, Ústav krizového řízení, Uherské Hradiště, Studentské nám. 1532, 686 01 Uherské Hradiště, e-mail: dvorakji@centrum.cz*
*Ing. Vladimír Šulc, Ph.D., Policejní akademie České republiky v Praze, Fakulta Bezpečnostního managementu, Ústav managementu a informatiky, Lhotecká 559/7, 143 01 Praha 4, e-mail: lada.sulc@seznam.cz*

pohled na chápání bezpečných procesů v řízení definovaných reálných systémů (organizací) a v novém prostředí a pojetí dynamicky se vyvíjejícího moderního soudního inženýrství.

Cílem [1] tohoto příspěvku je také moderní vymezení vzdělávání odborníků v oblasti kybernetické bezpečnosti v procesním inženýrství a dalších programech a také aktivní využití úloh budované Laboratoře aplikované kybernetické bezpečnosti (LAKB) pro magisterské studium na Fakultě logistiky a krizového řízení v Uherském Hradišti (FLKŘ) Univerzity Tomáše Bati ve Zlíně (UTB). Vedle již existující Laboratoře kybernetické bezpečnosti, navazující na tématiku procesního inženýrství, pro bakalářské studium, kde je cílem poskytnout studentům základní znalosti v oblasti vysokoškolských disciplín, zejména kybernetiky (kybernetických systémů, tj. v oblasti řízení a sdělování informace v technických a sociálně-technických systémech), kybernetické bezpečnosti, kyberprostoru kybernetických útoků a obrany systémů tj. také v oblasti tvorby a užití datových a stavových prostorů, zejména jejich systémové odolnosti proti kybernetickým útokům vycházejícím z Předpisu č. 181/2014 Sb., Zákona o kybernetické bezpečnosti. Základním cílem tohoto zákona je zvýšit bezpečnost kybernetického prostoru a ochránit tu část infrastruktury, která je pro fungování všech systémů podstatná a jejíž narušení by vedlo k poškození nebo ohrožení zájmu například i státu. Zákon stanovuje, jakým způsobem má být kybernetická bezpečnost zajištěna a určuje způsob reakce na kybernetické hrozby nebo řešení nastalého incidentu – a z toho přistupujeme k budování laboratoře aplikované kybernetické bezpečnosti. Uvedený požadavek [3] vyplývá také z postupně realizovaného usnesení a doporučení Bezpečnostní rady státu k návrhu společného minima pro potřeby vzdělávání v oblasti bezpečnosti a kybernetické bezpečnosti. Profilující této oblasti vzdělávání je znalost standardů v krizovém řízení, analýze rizik, odpovídajících právních norem, bezpečnostní politice a prevence kriminality, ochraně obyvatelstva, ekonomice krizových situací, aplikované informatice – cílem výuky je tedy poskytnout studentům znalosti o moderním zázemí ICT, umožnit jim pochopit **nové role kybernetiky** v řídící a rozhodovací činnosti a orientovat je především v produktech a nových technologiích. Poskytnout jim také potřebné praktické zkušenosti a efektivně kooperovat a komunikovat se specialisty z oblastí: zpracování dat, bezpečnosti počítačových a komunikačních sítí, dále také z oblastí bezpečnostní politiky a prevence kriminality (z mezinárodní dimenze bezpečnosti).

Informační a komunikační technologie (ICT) a nyní začínající znalostní společnost v nové ekonomice světa musí využívat především teoretické pojetí systémů a kybernetiky k vyjádření modelů reálných prostředí a vytváření vhodných modelů těchto prostředí s uvažováním struktur systémů (tj. vnitřního uspořádání prvků a podsystémů), chování systémů (tj. reakcí na podněty systémů a jejich reakce ve smyslu také časových proporcí uvnitř i vně těchto prostředí), podstatného okolí systémů v uvažovaném prostředí (tj. generátoru vstupních podnětů v časových relacích a také šumů (poruch a moderních nožných kybernetických útoků) jako součásti existence reálného pohledu na prostředí nás obklopující).

Současné zákonem vymezené samostatné obory informatiky a kybernetiky nám umožňují využití teoretického zázemí obou uvedených oborů a vyjádřit prostředky modelování v současném prostředí informatiky (digitálního prostředí) vhodného pro modely a jejich transformace za účelem modelování na výkonných číslicových počítačích a odpovídajících informací k získání například optimálních struktur systémů nebo jejich chování a u kybernetických systémů například ověření jejich stability v chování prostředí apod.

Základem poznání reálného prostředí je přesné vyjadřování procesů s vymezením vhodných rozlišovacích úrovní v nichž budou obsaženy také mezní stavy systémů jako existenčně nutná prostředí v reálných podmínkách s prostorem rizik a za dané dynamiky poznávaných procesů v existenci reálného prostředí s vymezenými mezními stavy a z nich odvíjejícího řízení (jako modelu kybernetického systému za podmínek obsáhlého vymezení rizik v reálném prostředí a také rizik informačních systémů například s ohledem na vysoce aktivní kybernetické útoky omezované současnými prostředky kybernetické bezpečnosti pro moderní reálné prostředí a tedy i nově získávanou představu systému (včetně kybernetických systémů v tomto reálném prostředí).

S tímto pohledem [4] můžeme procesy modelování vyjádřit matematicky jako *n*-rozměrné matice informací o systému a také v kybernetických systémech reprezentujících podsystémy reálného prostředí systémem (modelem systému), stavovými veličinami kybernetických systémů a podsystémů a dalšími maticemi časových relací.

Koncepce tohoto příspěvku je ve stručném vyjádření základních a nových pohledů na systémově vymezených procesech pro kybernetickou a informační bezpečnost v moderním kybernetickém prostoru budoucích „*učících se podniků a také organizací*“ ve znalostní ekonomice s podstatným okolím systémového chápání adaptabilního soudního inženýrství. Tento kybernetický pohled na procesní inženýrství bude také možným příspěvkem pro právní chápání, vedle již existujících fyzických a právních osob, nově diskutované v robototechnických systémech „*elektronické osoby*“ pro potřeby soudních znalců **v této oblasti rizikového managementu**.

## 2. SOUČASNÝ STAV ŘEŠENÉ PROBLEMATIKY

Smyslem výzkumu je především systémové vymezení procesů v kybernetické bezpečnosti a vyjádření procesů, jak ochránit tzv. informační aktiva – tedy prvky informačního systému (hardwarové komponenty, aplikační a systémový software, datové struktury atd.), které mají pro funkčnost informačních systémů (IS) a jeho provozovatele nezastupitelnou hodnotu. Na základě analýzy aktiv a jejich zranitelných míst vyjadřujeme, jak identifikovat možné bezpečnostní hrozby, které mohou napadnout konkrétní zranitelné místo konkrétního aktiva. Tedy popsat možnou hrozbu včetně možného zdroje hrozby, případně úmyslnost a motivaci útočníka, vliv hrozby na jednotlivé atributy informační bezpečnosti aktiva (dostupnost, integritu, důvěrnost). Součástí analýzy hrozby by měl být i odhad pravděpodobnosti, případě možné frekvence hrozby.

Situace, kdy se uvedená hrozba pokusí působit na zranitelné místo s cílem ohrozit informační bezpečnost aktiva, je již bezpečnostní událostí. Pokud se působením hrozby naruší vlastnosti aktiva natolik, že dojde k narušení informační bezpečnosti, vzniká pak bezpečnostní incident. Bezpečnostní incident je tedy stav aktiva a bezpečnostní událost aktivita, která k tomuto stavu vede. Kybernetické hrozby (kyberhrozby) jsou širokou veřejností vnímány především v oblasti možných finančních ztrát a zneužití

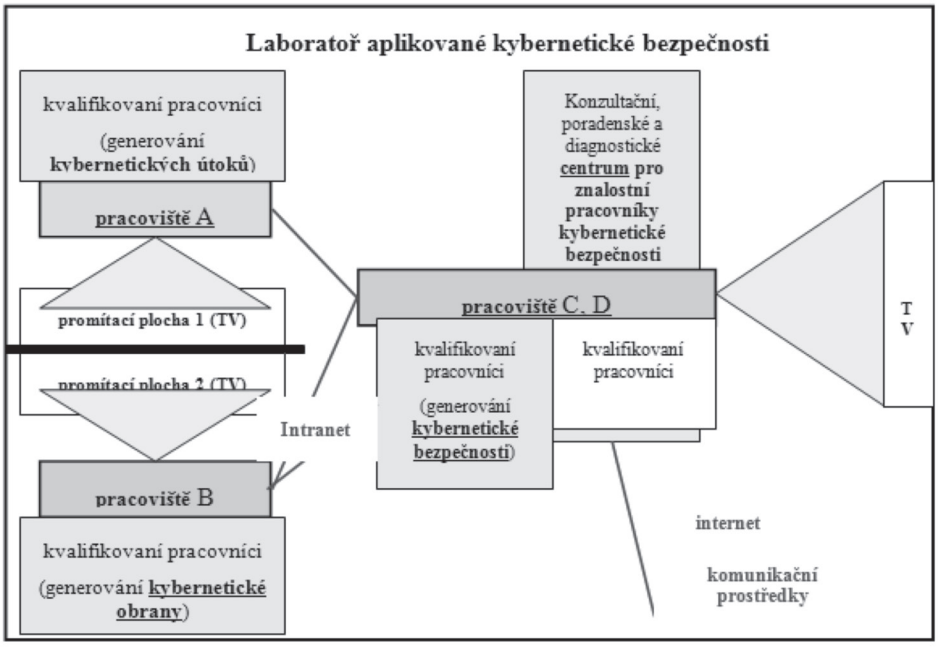
osobních dat; realita celé problematiky je ale mnohem širší a zahrnuje průmyslovou, vojenskou či politickou špionáž, aktivity organizovaného zločinu, politicky motivované šíření dezinformací či kybernetický terorismus (kyberterorismus).

Zabýváme se také vybranými technickými otázkami kybernetické bezpečnosti zahrnujícími řešení bezpečnostních incidentů subjektů spravujících důležité komunikační a informační systémy pro stát, možnou analýzu malware, sběrem typických stavů virtuálních modelů reálných systémů a vyhodnocováním informací o kybernetických útocích a hrozbách atp. [5], [6], [7]. Pomocí informačních kanálů jako jsou sociální sítě, webové noviny, rozhlas, TV, blogy, diskusní fóra, diskuze pod články lze s nebývalým úspěchem ovlivňovat obyvatelstvo cílové země. Výsledkem může být podlomení důvěry, morálky lidí cílové země a ideálně pak třeba i podpora protivníka k neprospěchu vlastní země. Takový pohled na vedení moderní války může být založen na teorii, že hlavním bojovým prostorem je mysl. Vedení nových konfliktů respektive válek nové generace bude zřejmě založen na válce informační a psychologické tak, aby bylo dosaženo nadvlády u nepřátelských vojsk, získána kontrola jeho zbraní, tj. aby nepřátelské ozbrojené síly a civilní obyvatelstvo bylo morálně a psychologicky zlomeno. Zřejmě pak hlavním bude kyberprostor, přes který lze velmi efektivně podporovat politické, ekonomické, ideologické i vojenské operace v reálném světě.

## 3. MOŽNOSTI A NÁVRHY SYSTÉMOVĚ VYMEZENÝCH PROCESŮ PRO LABORATOŘE KYBERNETICKÉ BEZPEČNOSTI (LAKB)

Moderní prostředí informační a také nově se rozvíjející znalostní společnosti bude stále více preferovat systémová a teoretická vymezení prostředí výzkumu a vzdělávání s cílem zachycení podstatného vlivu na existenci reálně definovaných systémů. Nová uskupení znalostního přístupu k celoživotnímu vzdělávání budou vymezována prostředím rizik odvíjejícími se od optimálních a stabilních systémů světa se svým reálným časem a v sociálně-technickém prostředí nazývaným kybernetickým prostorem (kyberprostorem) naplňujícím přijatý a realizovaný „*Kybernetický zákon*“. V zájmovém kyberprostoru musí být definovány systémově vymezené procesy pro nové technické a technologické úlohy transformací informací především v oblasti dnešních aplikací informačních a komunikačních systémů (ICT). Cílem vzdělávání bude osvojení si základních teoretických a vhodných praktických prostředků komunikace mezi systémy a pochopení moderních principů systémového a kybernetického přístupu k tvorbě modelů a modelování bezpečných reálných systémů, jejich diagnostikování a obnovy zejména při aplikacích moderního řízení na pozadí elektroniky a v budoucích projektech s umělou inteligencí spojených s rozvojem inženýrských přístupů pro zajímavou a potřebnou systémovou integraci na pozadí aktivní kybernetické bezpečnosti.

Zaměřujeme se především na pochopení rozvíjejících teoretických přístupů k moderní tvorbě modelu, modelování a projektování systémově vymezených úloh v kyberprostoru reálných systémů na pozadí aktivní kybernetické bezpečnosti. Jde především o pojetí: teorie modelů a modelování pro projektování adaptabilních prostředí znalostní společnosti, teoretické kybernetiky a metod technické kybernetiky pro sociálně-technické systémy a hrozby pramenící z online aplikací, teorie a aplikace diagnostiky útoků pro zvýšení kybernetické bezpečnosti systémů, možnosti aplikace teorie obnovy v procesech aktivní kyberbezpečnosti, užití metod operačního výzkumu pro optimalizaci kyberbezpečnosti z pohledu logistiky, procesního inženýrství, rizik a krizového řízení systémů, možnosti systémového řešení imunitního systému aktivního boje v technických konstrukcích projektů kyberbezpečnosti, kybernetická bezpečnost z pohledu zákona a vyjádřených teorií (kyberprostor, kritická informační struktura, bezpečnost informací, významný informační systém, významná síť, správce informačního




*Obr. 1 Model systémově vymezených procesů pro novou LAKB. (Zdroj: vlastní)*
*Figure 1 Model of systemically defined processes for new LAKB. (Source: own)*

a komunikačního systému, bezpečnostní opatření), možnosti aplikací metod umělé inteligence do modelů inteligentních systémů trénovacího prostředí kyberbezpečnosti a přípravy učícího se prostředí pro znalostní společnost, řízení bezpečnosti v procesech kybernetických útoků a ochrany dat (stavového prostoru systému), moderní robotické a bezpilotní prostředky a kyberprostor, jejich bezpečnost a jejich řízení a tvorba aktivních útoků těchto prostředků a jejich vhodná eliminace. Modelování kybernetického systému vhodnými prostředky matematického jazyka (měření úrovně a heterogenity dat a stavových prostorům, korelační a regresní analýza, faktorová analýza, predikce časových řad atd.).

Cílem moderní Laboratoře aplikované kybernetické bezpečnosti bude především na vysokoškolské úrovni poskytnout studujícím celoživotního vzdělávání znalostních pracovníků moderních „*učících se firem nebo organizací*" požadovaný integrující profil aplikované kybernetiky v rozsáhlém kyberprostoru bezpečnosti a to především cílevědomým rozvojem jejich znalostí teoretických disciplín. Především však v kybernetické bezpečnosti (v oblasti systémově vymezeném kyberprostoru určeném pro tvorbu a užití datových a stavových prostorů a jejich odolnosti proti kybernetickým útokům a všem dalším formám kybernetické války), systémům utajování citlivých informací a dat a užití moderní kryptografie (v oblasti bezpečné komunikace mezi systémy a zálohování struktur a chování rozsáhlých hierarchicky členěných dynamických systémů), vědy, výzkumu, inovací, vzdělávání a nových technologií a techniky (v oblasti vývoje nových a perspektivních technologií v oblasti ICT a širším okolí systémů v informační a znalostní společnosti a samozřejmě užití prostředků umělé inteligence).

Společným prostředím bude integrující směr daný teoretickou kybernetikou jako oboru pro řízení a sdělování informací v živých a technických objektech sjednocující uvedené oblasti a na základě systémového vnímání kybernetické bezpečnosti na:

**Pracoviště A:**

- je tvořeno dvěma PC (PC1 – počítač napojen na Internet, PC2 – napojen na Intranet laboratoře tj. propojení všech pracovišť celé laboratoře),
- studující tvoří kvalifikovaní pracovníci vytvářející na PC2 vhodnými prostředky *generování kybernetických útoků* na pracoviště A a to za pomoci kyberšpionáže a dalších prostředků kybernetiky určených pro rozpoznávání scény předpokládaného kybernetického incidentu (zadávaného a řízeného z pracoviště C – reprezentované kvalifikovanými vědeckými a pedagogickými pracovníky),
- společná scéna je zobrazena projekcí přes vhodný dataprojektor na promítací plátno 1 (nebo přímo zobrazena na velkoplošné TV),
- situace pracoviště A je zobrazeno na monitoru PC a také na pracovišti C (určené pro řízení kybernetické bezpečnosti v kyberprostoru reprezentovaných kybernetických útoků a obrany – generovaných na pracovištích A a B).

**Pracoviště B:**

- je tvořeno dvěma PC (PC1 – počítač napojen na Internet, PC2 – počítač napojen na Intranet laboratoře tj. propojení všech pracovišť laboratoře),
- studující tvoří kvalifikovaní pracovníci vytvářející na PC2 vhodnými prostředky – *generování kybernetické obrany* na pracoviště B a to za pomoci kyberšpionáže a dalších prostředků určených pro rozpoznávání scény předpokládaného kybernetického incidentu,
- společná scéna je zobrazena projekcí přes vhodný dataprojektor na promítací plátno 2 (nebo situace kybernetické obrany je přímo zobrazena na velkoplošné TV),
- situace pracoviště B je zobrazeno na monitoru PC a také na pracovišti C (určené pro řízení kybernetické bezpečnosti v kyberprostoru reprezentovaných kybernetických útoků a obrany a generovaných na pracovištích A a B).

**Pracoviště C:**

- je tvořeno dvěma PC (PC1 – počítač napojen na Internet, PC2 – počítač napojen na Intranet laboratoře tj. propojení všech pracovišť laboratoře),
- kvalifikovaní pracovníci pracoviště C vytvářejí na PC2 vhodnými prostředky – *zadávání školních* úloh na procvičování kybernetických útoků a obrany a řídí tento proces incidentu tak, že:
  - učiní společně s pracovníky pracovišť A a B závěry k účinné kybernetické bezpečnosti (školního příkladu nebo řešeného projektu pro reálné prostředí) a prezentuje se na pracovišti C,
  - poskytne celý algoritmus kybernetické bezpečnosti do báze znalostí na pracovišti D,
- společná scéna je zobrazena projekcí přes vhodný dataprojektor na promítací plátno nebo přímo na velkoplošný TV,
- situace pracoviště C je zobrazována průběžně ze všech pracovišť laboratoře a to jako zpětnovazební informace pro dokonalé řízení celého procesu incidentu v časových měřítcích kvalifikovaných pracovníků a práce celé sítě počítačů v reálném čase,
- přímá komunikace s NCKB a dalšími orgány KB mezinárodního a národního charakteru (konzultace k řešeným úlohám a aktivní účast na aktivitách – kurzech a celoživotním vzdělávání pracovníků),
- publikační činnost.

**Pracoviště D:**

- je tvořeno dvěma PC (PC1 – počítač napojen na Internet, PC2 – počítač napojen na Intranet laboratoře tj. propojení všech pracovišť laboratoře),
- konzultující jsou kvalifikovaní pracovníci vytvářející na PC2 další možné úkoly pro řešení případových studií, náměty na poradenské aktivity tohoto centra a dále podněty pro operativní strukturování znalostní báze pro potřeby diagnostikování příčin krizových situací,
- společná scéna je zobrazena projekcí přes vhodný dataprojektor na další promítací plátno (nebo na velkoplošnou TV),
- situace pracoviště D je zobrazeno na monitoru PC a také na pracovišti C (pracoviště určené pro řízení kybernetické bezpečnosti v kyberprostoru probíhajících kybernetických útoků a obrany),

- pracoviště C odpovídá na činnost celé laboratoře a za procesy podléhající utajovaným skutečnostem.

## 4. DISKUSE

Na základě uvedené systémové koncepce možného řešení reálného prostředí představovaného systémem a odpovídajícími modely jsou vytvořeny základní možnosti, že iteračními kroky lze zpřesňovat uvedené modely studia i model LAKB se svými podsystémy pomocí simulací. Předpokládáme také, že uvedené kroky adaptací nám pomohou vytvářet základnu pro možné návrhy k současným právním normám a také prostředí LAKB může přispět k procesům poznání dynamiky kybernetické bezpečnosti a také rozšířit zajímavou oblast soudního inženýrství.

Z hlediska znaleckého byla uvedená koncepce LAKB řešena tak, že podle potřeb bude se postupně vytvářet v odpovídajících pracovištích C a D (báze znalostí pro řešené modely aplikované KB) a tím naplňovat také zájmové obory kriminalistiky, bezpečnosti a dalších oborů v souladu s vyhláškou č. 123/2015 Sb. a tím také vytvářet vhodné a předpokládané zařazení vybraných odborníků podle seznamu znaleckých oborů a odvětví určených pro výkon znalecké činnosti znalců. Postupně vyvářená báze umožní práci s informacemi jak fyzických osob, tak i znaleckých ústavů v oborech například: informační technologie, informatika, kriminalistika, kybernetika, spoje, telekomunikace, výpočetní technika a případně další v souladu s přílohou č. 2 uvedené vyhlášky.

Využití LAKB vidíme také v možnosti:

- aktivní spolupráce znalců s pedagogickými pracovníky fakult na zkvalitnění výuky a řešení případových studií, ve spolupráci při oponování prací studentů a studujících mladých vědeckých pracovníků v oblasti KB (doktorských disertačních prací),
- řešení a konzultací vědeckých úkolů na fakultě UTB ve Zlíně a PA v Praze,
- výměně zkušeností na plánovaných odborných konferencích v Uherském Hradišti a Brně s cílem vytváření odborných týmů v oblastech modelování KB a odborných oborů znalců LAKB poskytne řadu námětů k řešení dílčích úloh z praxe a bude aktivně pomáhat všem uvedeným odborníkům ve využívání moderních metod umělé inteligence (znalostní báze).

## 5. ZÁVĚR

Stručné vyjádření uvedeného systémového pojetí při řešení výzkumu úkolu dává především tyto předběžné závěry:

- v pojetí systémového přístupu k promyšlenému vyjádření modelů z procesního pohledu dává náměty pro rozvoj potřebných prostředků kybernetiky včetně aplikovaných směrů i v soudním inženýrství,
- vyjádření kybernetické bezpečnosti jako uvedeného modelu procesního inženýrství dává také ucelený pohled i zde na možnost užití stavových veličin v procesech ukládání dat ve prospěch simulačních procesů a také pro budoucí nové pojetí a užití prostředků umělé inteligence a moderní pojetí tvorby znalostní báze pro oblast kybernetické bezpečnosti.

Koncepce tohoto příspěvku je ve stručném vyjádření základních a nových pohledů na možné celoživotní vzdělávání znalostních pracovníků „*učících se podniků a organizací*“ použitelné i v současných oblastech soudního inženýrství. Jsou zde vyjádřeny systémově vymezené procesy pro kybernetickou a informační bezpečnost v moderním kybernetickém prostoru znalostní ekonomiky s podstatným okolím také možného systémového chápání adaptabilního soudního inženýrství a uvedena představa možné laboratoře **výuky aplikované kybernetické bezpečnosti** a předpokládáme také i pro potřeby soudních znalců v této oblasti rizikového managementu.

Tento příspěvek byl podpořen úkolem „Využití *ICT a matematických metod při řízení podniku*“ 31.12.2014/VUT, tematická část tohoto projektu (Dvořák a kol.: „*Systémově integrované prostředí pro návrh inteligentních modelů, modelování a simulací moderního kyberprostoru podniku*“) Interní grantové agentury Vysokého učení technického v Brně s registračním číslem FP-S-13-2148 a zároveň také projektu dílčího vědecko-výzkumného úkolu č. 1/1 „*Možnosti využití nových technologií s důrazem na zefektivnění a urychlení činnosti orgánů činných v trestním řízení a dalších subjektů*“ Policejní akademie ČR v Praze, 2016.

## 6. LITERATURA

[1] DVOŘÁK J., KONEČNÝ J., JANKOVÁ M.: Možnosti identifikace útoků v kyberprostoru krizového řízení. In: *Krizové řízení a řešení krizových situací 2015.* Univerzita Tomáše Bati ve Zlíně, Uherské Hradiště, 2015. s. 64–69. ISBN 978-80-7454-573-3

[2] JANKOVÁ M.: Rozvoj moderního managementu v kyberprostoru užití ICT. In: *Hradecké ekonomické dny 2015.* Gaudeamus, Hradec Králové, 2015. s. 305–311. ISBN 978-80-7435-546-2

[3] JANKOVÁ M., DVOŘÁK J.: Možnosti rozpoznávání rizik v ekonomické kybernetice. In: *Krizový management 2014.* Ed.: doc. Ing. Miloslav Hub, Ph.D., Univerzita Pardubice, Pardubice, 2014. s. 12–19. ISBN 978-80-7395-871- 8

[4] JANKOVÁ M.: *Internetové nástroje pro celoživotní vzdělávání v sektoru IT*. Vysoké učení technické v Brně, Fakulta podnikatelská, Brno, 2016. 234 s.

[5] POŽÁR J.: *Informační bezpečnost*. Aleš Čeněk, Plzeň, 2005. ISBN 80-86898-38-5

[6] SMEJKAL V.: *Právo informačních a telekomunikačních systémů*. 2. aktualiz. a rozš. vyd. C. H. Beck, Praha, 2004. ISBN 80-247-0058-1

[7] SMEJKAL V., RAIS K.: *Řízení rizik ve firmách a jiných organizacích*. Grada Publishing, a.s., Praha, 2013. 466 s. ISBN 978-80-247-4644-9